Pseudonymous Proxy Server ("PPS"): Figures & Examples:

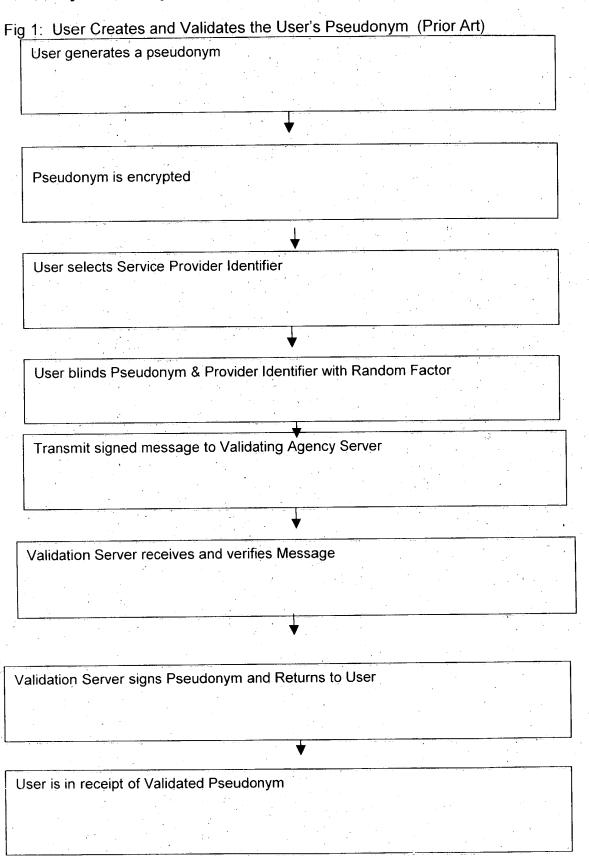
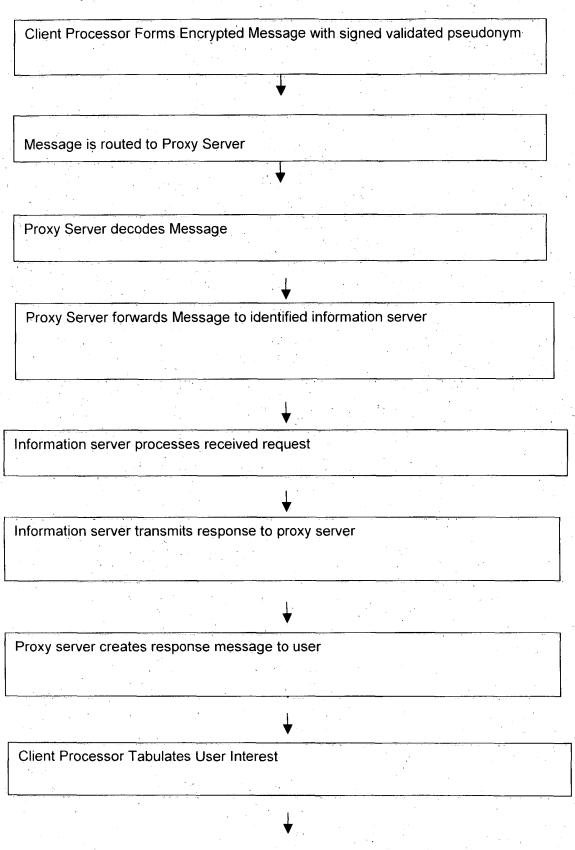


Fig 2: Pseudonymized Message is Routed through Proxy Server which Re-Identifies the Pseudonymized Data, Routes the Re-Identified Message to the Information Server and Routes Response to User (Prior Art)



Client Processor Transmits Message to Proxy Server to Update Profile Interest Summary

Fig 3: User Creates and Validates the User's UID that can be used as a Pseudonym and ACRS that govern the User's Access to Actual vs. Pseudonymous Data.

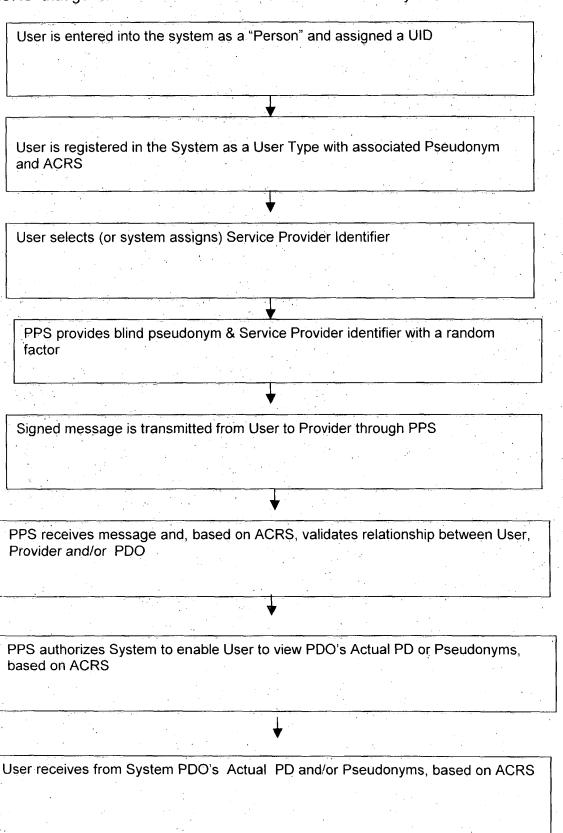


Fig 4: Pseudonymized Message is Routed through Proxy Server which Re-Identifies the Pseudonymized Data, Routes the Re-Identified Message to the Information Server and Routes Response to User in the form of Actual or Pseudonymous Data, based on the ACRS.

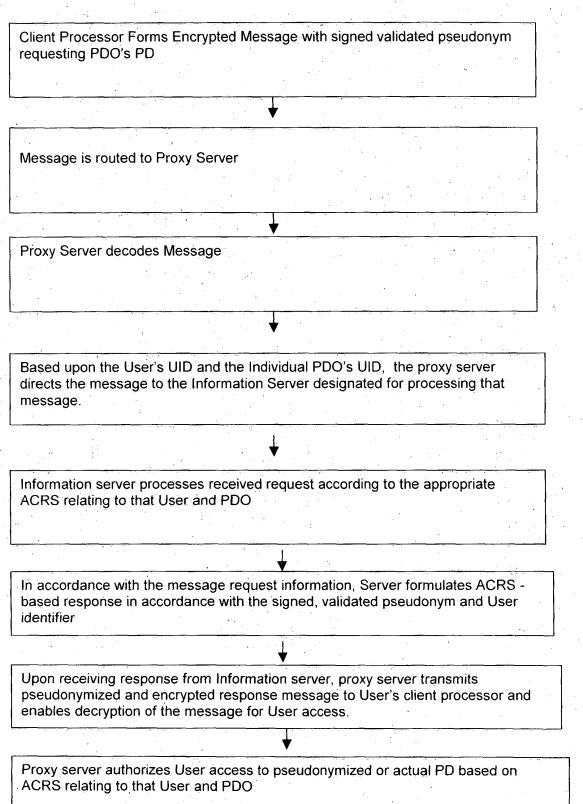


Fig 5:
User Requests Private Data (PD). Pseudonymous Proxy Server (PPS): 1. identifies User by UID or UNID; 2. Validates request; and 3. grants User access to Actual or Pseudonymous data, in accordance with the ACRS implemented by the PPS, which is also known as the UID – ACRS controller.

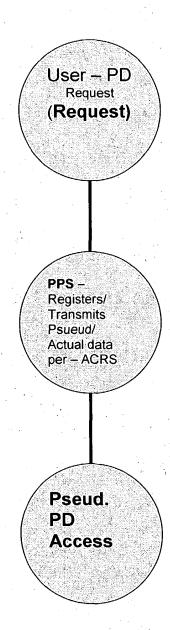


Figure 6.:

UID-ACRS Controller is a form of PPS that can be implemented to control UID's and ACRS among multiple servers in a "Hub and Spoke" network configuration. The UID-ACRS Controller maximizes control over all Individual UID assignments and Users' ACRS to maximize security, privacy and accountability when the User accesses Private Data (pseudonymous and actual per the ACRS)

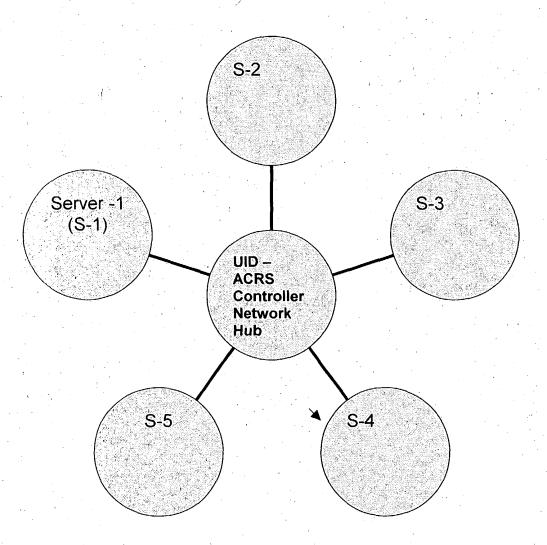
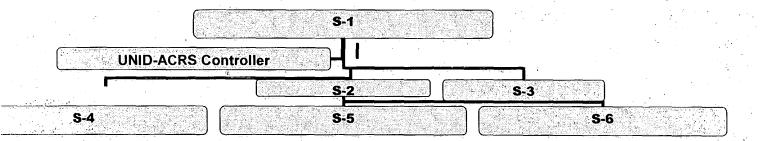
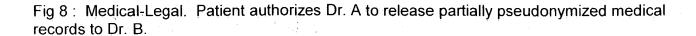


Figure 7.: Multicast/ Computer Network Tree with UNID-ACRS Controller

UNID-ACRS Controller is a form of PPS that can be implemented to control UID's and ACRS among multiple servers in a "Network Tree" configuration. The UNID-ACRS Controller maximizes control over all Individual UID assignments and Users' ACRS throughout all Servers in the Network Tree to maximize security, privacy and accountability when the User accesses Private Data (pseudonymous and actual per the ACRS)





Dr. A – Server 1 – Maintains Patient's Medical record with ACRS governing access for Dr. A's staff and limited access for Patient

Patient routes message to Dr. A with signed Authorization to release records attached, requesting that Dr. A grant access to Patient's medical records to Dr. B

Proxy Server codes Message to Pseudonymize identity of Dr. B. Dr. A's ACRS replaces Dr. B's name with a Pseudonym.

Based upon the service provider identifier associated with the message, the proxy server forwards the message to Dr. B (or an identified information server - Server - S 2 designated by Dr. B and synchronized with Dr. A's server per ACRS)

Information server processes request and grants ACRS to Dr. B in accordance with Authorization granted by Patient (e.g. release everything but address and social security number)

In accordance with the message request information, Server forwards the message to Dr. B with ACRS -based pseudonymization of PD

Dr. B logs onto the system which identifies Dr. B as a User with the appropriate ACRS as granted to Dr B by Patient.

Dr. B accesses Patient's Medical Records with specific PD pseudonymized in accordance with Dr. B's ACRS.